(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 271 418 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.01.2003 Bulletin 2003/01

(51) Int Cl.[7]: **G07C 9/00**, G07B 15/00

(21) Application number: **01115474.7**

(22) Date of filing: **27.06.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Nokia Corporation**
02150 Espoo (FI)

(72) Inventors:
- **Bunte, Björn**
  44795 Bochum (DE)
- **Krummel, Holger**
  44789 Bochum (DE)
- **Bollmann, Tilman**
  45131 Essen (DE)

(74) Representative: **Becker Kurig Straus**
Patentanwälte
Bavariastrasse 7
80336 München (DE)

(54) Method for accessing a user operable device of controlled access

(57) Method for accessing a user operable device having a limited access ability by a user. Therefore a user transmits an inquiry using a mobile device via a wide area transmission network to a key authority. The key authority retransmits an electronic access key. This access key is stored in the mobile device and later transmitted to a controller unit controlling the access the user operable device allowing the user to operate on it.

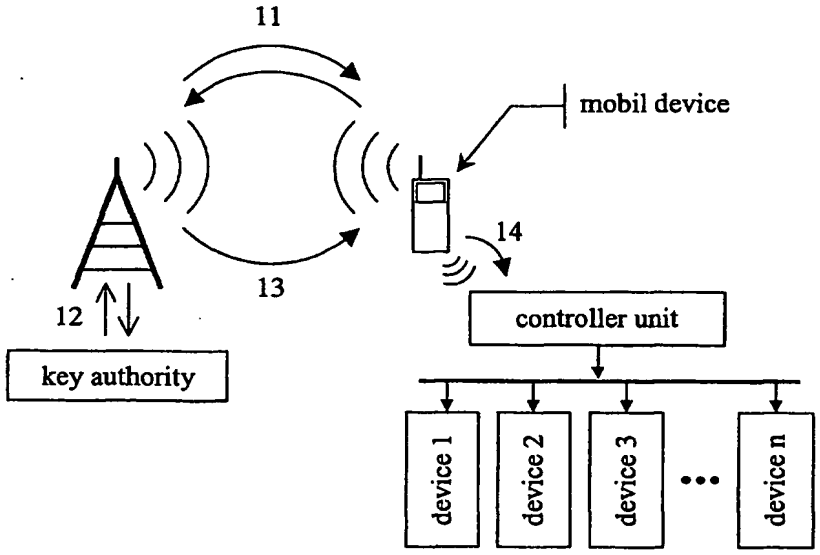

Fig. 1

EP 1 271 418 A1

Description

[0001] The present invention relates to a method for accessing a user operable device of controlled access. In particular, the invention relates to a method for accessing a user operable device of controlled access secured by an electronic key which can be assigned by radio link.

[0002] Traditionally, the access to several devices, particularly devices which can be rented, is often limited by time restraints due to the fact, that for example a real key must be handed over to the user wanting to rent this device. Therefore, local agencies have to be maintained, which are cost-intensive. To operate such services from a central office without local agencies it is necessary to organize the rental process without handing over physical objects such as a real key.

[0003] The object of the present invention is to provide a method for accessing a user operable device having a limited accessibility by a user.

[0004] A further object of the present invention is to provide a mobile device used to request access to the user operable device granted by a key authority for permitting access and used to transmit the permission of access to a controller unit controlling the access to the user operable device.

[0005] A further object of the present invention is to provide a controller unit in order to control the access to the user operable device of limited access.

[0006] The object of the present invention is solved by claim 1. In accordance with the present invention there is provided a method for accessing a user operable device of a limited accessibility by a user comprising transmitting an inquiry from a mobile device of said user to a key authority via a wide area transmission network in order to obtain an access key for accessing functions of a controller unit of said user operable device, verifying said inquiry by said key authority, assigning said access key by said key authority, transmitting said access key via a wide area transmission network to said mobile device, storing said access key in said mobile device, transmitting said access key form said mobile device to said controller unit via a local area transmission network, validating said access key and granting access to said user operable device.

The solution of the object is attained by the possibility of using an electronic key to operate devices. Thus, granting access to these devices can be done without any physical contact. Therefore, the presented method comprises an inquiry step in which the user defines the device desired to operate on and the conditions under which the device shall be operated via a wide area transmission network using a mobile device. A key authority verifies this inquiry. When permission of usage can be given to the user an access key is transmitted via a wide area transmission network to the mobile device. The mobile device has the possibility to store this access key for later usage. When desired by the user the access key is transmitted via a local area transmission network to a controller unit controlling the user operable device which was determined by the user's inquiry. The controller unit validates the access key and grants access to the user operable device.

[0007] Preferably, the method comprises a step of transmitting information back concerning the validity of the access key via the local area transmission network to the mobile device of the user in order to inform the user about the granting process and conditions including for example a confirmation of validity, a validity time of the access key and a number of possible accesses. Additionally, the transmission back can also include information concerning the operable functions which are accessible by the user. This is an important information since not all devices controlled by the controller unit need to be user operable.

[0008] Conveniently, the inquiry step of the method according to the present invention can include several transmissions and retransmissions of additional data. For example, additional data including offers made by key authority according to a first inquiry of the user, a selection of offers by the user and also information about the conditions under which assigning of the access key is possible. If the user desires to use a kind of device without defining the exact type, the key authority is able to transmit an information about several operable devices according to the type defined by the user's inquiry. For example, if the user desires to rent a car, the car rental can offer him different cars and additionally different built-in equipment like a mobile phone. The user selects an offer transmitted to the key authority which relates to the car rental in this case.

[0009] Preferably, the user transmits a desired period of time defining the period of validity of the access key. In case of the car rental examples, usually the user defines the number of days for using the car.

[0010] A preferable embodiment includes transmitting and verifying identification data of the user. Additionally, payment information are also transmitted and verified. Payment information can be credit card information or bank account information.

[0011] Conveniently, the key authority is a service provider. Additionally, the key authority is a call center. Preferably, the key authority is a WEB server accessed via a WEB page or the key authority is a WAP server accessed via a WAP page.

[0012] A controller unit can control the access to several functions of the user operable device. Due to this it is necessary to provide selective access to single user operable functions of the device which can be performed using different access keys for the different user operable functions. Additionally, the user operable functions are sorted in a hierarchical structure. The position in the hierarchical structure can be obtained and defined by the kind of function, the importance, the access security level and the like of the operable device. According to the hierarchical structure of the operable devices

it is possible to define a corresponding access key structure. This means that a level is assigned to each access key and an access key of a certain level includes the accessibility to all user operable devices of corresponding access keys with lower key levels. This kind of access can be interesting for maintenance of devices. Therefore, access keys can be provided for example by the manufacturer or any other service provider offering maintenance services.

[0013] A possible implementation of a hierarchical access key structure is providing keys for towing service. In case of a brake down of a car the owner has to call the towing service and has to wait until the car is brought for example to a parking area of a garage. A lot of time gets lost. In order to shorten the time spent by the user for the towing process it is possible according to the method of the present invention to submit an access key to the towing service enabling to open the car, switch on electrical devices like lights, flash lights and the electrical system of the car but not to start the engine of the car, use the built-in devices like mobile phone or open the boot of the car. The submitted access key shall only allow the towing service provider to tow the car to a garage and therefor needed functions of the car are allowed to use. Later an other access key of an higher level can be provided by the owner to the garage to make it possible for the mechanics to use the same functions like the towing service and additionally to operate on the electrical system of the car like reading out management data, status data, error messages of the engine or programming the management system. Even the higher level access key provided to the garage must not allow the usage of built-in devices like a mobile phone.

The different access key need not be provided by the owner of the car himself. It is possible that the owner of the car uses the service of a key authority providing the different access key to the towing service or the garage according to the method of the resent invention.

[0014] Another implementation of a hierarchical access key structure is providing key for access to terminals. Computer access is a typical system using access keys of a hierarchical structure. A local terminal is equipped with a Bluetooth receiver. To gain access to the terminal an access key according to the method of the present invention is transmitted to the receiver logging on the user of the mobile device. According to the permission of the user different access levels of the computer terminal are granted to the user.

[0015] Preferably, a device identification of the user operable device is co-coded in the access key to provide the access to a defined device. Additionally, a period of validity of a total access period is co-coded. To increase the security of the access process a period of validity of a first access can conveniently be also co-coded. And the possibility of co-coding the number of access procedures is also provided.

[0016] Additionally, validating of the access key by the controller unit can be performed by comparing with a validation key generated by the controller unit. The generation of a key comprises several additional parameters according to the fact that the access key can include co-coded information such as period of validity, number of accesses. These additional parameters have to be provided to the generation process.

[0017] Preferably, instead of comparing the access key with a generated key a reference key can be used which is transmitted to the controller unit via an interface. The usage of a reference key for the validation step is more reliable since a generation method of a key can be revealed or discovered and therefore the key authority can be bypassed. Conveniently, the reference key is stored in the controller unit.

[0018] To use a stored key to compare with the access key is a further preferable method to validate the access key. Particularly, the latter method is useful when keys for maintenance access shall be provided. It is obviously possible to delete stored keys in order to prevent further usage of a certain access key.

The possibility of transmitting a key to be stored in the controller unit for example offers the opportunity to an owner of a car to provide an access key to a second person for using his car. In this case the owner of the car is the key authority who receives the inquiry, verifies the information provided by the inquiry step and transmits the access key to grant access to his car to a second person.

[0019] Additionally, the reference key transmitted via the interface unit or a stored key need not to be used directly in the validating step. It is also possible to use the reference key or the stored key as part of the data used for generating the validating key.

[0020] In order to prevent misappropriation and misuse of the access key all transmission steps are secured by using encrypted transmission. Additionally, encrypted transmission used for the inquiry step can also enhance the security of the method particularly when user identification or payment data are transmitted.

[0021] Preferably, the local area transmission network is a low power radio frequency network. Conveniently, the local area transmission network may be a radio frequency network according to e.g. the Bluetooth standard. Alternatively, the local area transmission network may be an infrared transmission network.

[0022] Preferably, the wide area transmission network is a network for mobile transmission and communication such as GSM, UMTS or the like. Conveniently, the wide area transmission network is a cellular network for mobile communication. Specifically, the wide area transmission network is a mobile data transmission and communication network according to the GSM standard. More specifically, the wide area transmission network is a mobile data transmission and communication network according to the WCDMA standard. Most preferably, the wide area transmission network is a mobile data transmission and communication network accord-

ing to UTMS standard.

[0023] Additionally, the access key is transmitted via a message according to e.g. the SMS standard included in the GSM standard.

[0024] The present invention further comprises a mobile device according to the above discussed method. This mobile device comprises the following means in order to fulfil the demands defined by the method of the present invention : a unit for inputting inquiry data to be transmitted to the key authority, a unit for transmitting the inquiry data via the wide area transmission network, a unit for receiving the access key, a unit for storing the access key and a unit for transmitting the access key to the controller unit.

[0025] According to the above explained method the mobile device can additionally comprise a unit for receiving information concerning the validity of the access key or the operable functions which are accessible by the user.

[0026] Preferably, to secure the access granted to the user by the key authority a re-coding of the access key is performed using information or data only accessible by the mobile device or the user thereof, wherein the data can be a PIN code only known by the user or a unique built-in mobile device identification.

[0027] Conveniently, a WEB client or a WAP client can be included in the mobile device.

[0028] The present invention further comprises a controller unit for usage in a method according to any one of the preceding claims and connectable to a user operable device comprising a unit for receiving an access key via a local area transmission network, a unit for storing the access key, a unit for validating the access key and means for controlling functions of the user operable device.

[0029] According to the above described method the controller unit can additionally comprise a unit for generating a validation key. Preferably, the controller unit comprises a unit for storing a key or several keys.

Conveniently, the controller unit comprises a unit for retransmitting information concerning the validity of the access key or the operable functions which are accessible by the user.

[0030] Preferably, the controller unit comprises an interface unit. This interface unit can be connected to an authorized device or an authorized instant. The connecting of the interface unit to an authorized device can be done using a common communication standard based on methods using wire for communication or wireless communication. More preferably, the interface unit uses a wide area communication network such as defined above. Additionally, the interface unit can also use a local area communication network defined above.

[0031] When using co-coded access keys additional units may be necessary to gain the additional data for generating the according validation key or for validating the co-coded information of the access key. These units could be units providing a clock signal for checking a period of time, device identification, for example the type of a unique number, a position signal e.g. a GPS signal or signals generated by the user operable device like notifying failure, misoperation or maintenance requirement.

[0032] The method according to the present invention provides a secure method to offer and to control access to user operable devices using a electronic key. The electronic key is provided by a key authority. In order to get a granted access to a desired user operable device an inquiry has to be transmitted by the user to the key authority including all necessary data and information. The electronic key is transmitted to a mobile device of the user used before to transmit the inquiry. The electronic key allows the user to get access to the user operable device which is controlled by a controller unit.

[0033] The present invention is described with respect to particular exemplary embodiments thereof and reference is accordingly made to the drawings in which:

- Fig. 1 illustrates schematically the sequence of information transmitted according to the method of the present invention,
- Fig. 2 shows a set of possible units included in a preferable embodiment of the controller unit,
- Fig. 3 illustrates the method of the present invention taking a procedure of a rental of a car as example.

[0034] Fig. 1 illustrates schematically the sequence of information transmitted according to the method of the present invention as also devices and units involved and visible for the user.

[0035] The first step of the method referenced as inquiry 11 comprises at least one inquiry to operate a certain device 1,2,3 or n. Commonly, the inquiry includes several transmissions and retransmission 11, 12. The key authority 12 is accessed via a wide area transmission network, particularly a GSM cellular network. Information about the user identification and payment data have to be verified. A positive verification leads to the transmission 13 of the access key of the user operable device to the mobile device which is stored in said mobile device. The access key stored in the mobile device and information about the user operable device transmitted from the key authority enables the user to identify the assigned user operable device. The transmission of the access key to the controller unit via a local area transmission network, like Bluetooth, allows the user to operate on a single or several devices controlled by the controller unit under the conditions co-coded in the access key.

[0036] Fig. 2 shows a set of possible units included in a preferred embodiment of the controller unit. Validating of the access key comprises several steps and can be carried out in different ways. Following reference numbers 21 to 24, shown in Fig. 2, the access key is transmitted 21 from the mobile device via a local area trans-

mission network to a receiver unit of the controller unit. If necessary, the access key can be stored in an access key buffer or passed directly 22 to the validation unit. The access key is validated thereon. A positive validation is passed 23 to a controlling unit responsible for controlling the user operable devices. The user operable devices are controlled via a controlling bus 24.

[0037] A co-coded period of validity in the access key has to be extracted 25 and monitored 26. When the period is run out the permission of usage expires and the user operable devices are no longer accessible.

[0038] There are different ways conceivable to validate the access key. The embodiment according to Fig. 2 shall describe different ways without limiting the validation process illustrated by using different line styles.

[0039] The validation of the access key is often done by comparing the transmitted access key with a validation key generated within the controller unit (follow reference numbers 30 to 32 shown in Fig. 2). To generate the validation key parameters like at least the device identification data have to be passed 30 to the validation key generator. The generated validation key is finally passed 23 to the validation unit.

[0040] Alternatively, a validation key can also passed 33 from a permanent or programmable key storage to the validation unit. Preferably, the key storage comprises a storage of data used 34 as additional parameters for the key generation. Additionally, an interface can provide access to the validating unit by providing a reference key in order to be compared with the access key. This reference key can also be stored 41 in the key storage or be used as parameter in the key generation comparable to a stored key. Such an access to the interface has to be controlled strictly since keys used in the validation step can be transmitted to the controller unit in order to overcome the key authority. However, if the interface is connected to a transmission network 40 providing access to the key authority the key authority, is able not only to transmit the access key to the user but also the corresponding reference key or part of the key to be generated in order to enhance the security of the method. Due to the additional transmission of data to the controller unit users are not able to pass the key generation since they lack important data.

[0041] Fig. 3 shows a possible course of a car rental process using the method according to the present invention. In a first step the users sends a first transmission for inquiry of a car to a car rental. The car rental responds to the request of the user offering several possible cars of different type, model and equipment. The user selects a car and desired additional equipment, defines the period of validity and transmits this information to the car rental. Subsequently the car rental transmits a request to the user to send an identification and information concerning the payment. This request has also to be answered by transmitting an identification number of the passport and credit card data to the car rental. All these data have to be verified by the key authority before an access key can be granted to the user.

A positive verification of the information given by the user leads to a transmission of an access key and additional information about the car like car number and parking lot number. The access key is stored in the mobile device. When the user wishes to get access to the car, he transmits the stored access key to the car. The access key can also enable the access to additional equipment of the car like a built-in mobile phone.

Claims

1. A method for accessing a user operable device having a limited accessibility by a user comprising the following steps:
   - transmitting an inquiry from a mobile device of said user to a key authority via a wide area transmission network in order to obtain an access key for accessing functions of a controller unit of said user operable device,
   - verifying said inquiry by said key authority,
   - assigning said access key by said key authority,
   - transmitting said access key via a wide area transmission network to said mobile device,
   - storing said access key in said mobile device,
   - transmitting said access key via a local area transmission network to said controller unit,
   - validating said access key in said controller unit,
   - granting access to said user operated device.
2. A method according to claim 1, wherein said controller unit transmits information back concerning the validity of said access key via said local area transmission network to said mobile device.
3. A method according to any of the preceding claims, wherein said controller unit transmits information back concerning operable functions which are accessible by said user.
4. A method according to any of the preceding claims, wherein said inquiry to said key authority includes several transmitting and retransmitting processes.
5. A method according to any of the preceding claims, wherein said inquiry to said key authority includes transmitting a desired period of time defining the period of validity of said access key.
6. A method according to any one of the preceding claims, wherein said inquiry to said key authority includes transmitting and verifying identification data of said user
7. A method according to any one of the preceding

claims, wherein said inquiry to said key authority includes transmitting and verifying payment information.

8. A method access according to any of the preceding claims, wherein said inquiry to said key authority includes transmitting and verifying credit card data.

9. A method access according to any of the preceding claims, wherein said inquiry to said key authority includes transmitting and verifying bank account data.

10. A method according to any of the preceding claims, wherein said key authority is a service provider.

11. A method according to any of the preceding claims, wherein said key authority is a call center operated manually or operated automatically by a voice assistant.

12. A method according to any of the preceding claims, wherein said key authority is a WEB server and accessed via a WEB page.

13. A method according to any of the preceding claims, wherein said key authority is a WAP server and accessed via a WAP page.

14. A method according to any one of the preceding claims, wherein said different access keys enable limited access to single functions of said controller unit.

15. A method according to any one of the preceding claims, wherein different keys are sorted hierarchically according to hierarchically sorted functions of said controller unit.

16. A method according to any one of the preceding claims, wherein a device identification is co-coded in said access key.

17. A method according to any one of the preceding claims, wherein a period of validity of a total access period is co-coded in said access key.

18. A method according to any of the preceding claims, wherein a period of validity of a first access period is co-coded in said access key.

19. A method according to any of the preceding claims, wherein a number of access procedures is co-coded in said access key.

20. A method according to any of the preceding claims, wherein a validation key is generated by the controller unit in order to compare said access key with said validation key during the validating step.

21. A method according to any of the preceding claims, wherein a reference key is transmitted directly from said key authority to said controller unit via an interface.

22. A method according to claim 21, wherein said reference key is stored in the controller unit.

23. A method according to claim 21, wherein said reference key is part of the data used for generating said validation key.

24. A method according to any of the preceding claims, wherein a key is stored in the controller unit in order to compare said access key with said stored key.

25. A method according to claim 23, wherein said stored key is part of the data used for generating said validation key.

26. A method according to any of the preceding claims, wherein transmitting is secured using encrypted transmitting methods.

27. A mobile device for usage in a method according to any one of the preceding claims, comprising:

- a unit for inputting inquiry data to be transmitted to said key authority,
- a unit for transmitting said inquiry data to said key authority via said wide area transmission network,
- a unit for receiving said access key assigned by said key authority and transmitted via said wide area transmission network according to any of the claims,
- a unit for storing said access key,
- a unit for transmitting said access key stored in the mobile device to said controller unit via said local area transmission network according to any of the claims.

28. A mobile device according to claim 27, comprising additionally a unit for receiving information concerning the validity of said access key.

29. A mobile device according to claim 27 or 28, comprising additionally a unit for retransmitting information concerning operable functions which are accessible to said user.

30. A mobile device according to any of the claims 27 to 29, comprising additionally a unit for recoding said access key.

31. A mobile device according to any of the claims 27

to 30, comprising a WEB client.

32. A mobile device according to any of the claims 27 to 31, comprising a WAP client.

33. A controller unit for usage in a method according to any of the preceding claims and connectable to a user operable device, comprising:

- a unit for receiving an access key via a local area transmission network,
- a unit for validating said access key transmitted by said mobile device,
- means for controlling functions of said user operable device to which the access is granted by the verified access key.

34. A controller unit according to claim 33, comprising additionally a unit for generation of a validation key to be compared with said access key by the validation unit.

35. A controller unit according to claim 33 or 34, comprising additionally a unit for storing said access key.

36. A controller unit according to any of the claims 33 to 35, comprising additionally a unit for storing a key or several keys used for the validating step.

37. A controller unit according to any of the claims 33 to 36, comprising additionally a unit for retransmitting information concerning the validity of said access key or information concerning operable functions which are accessible by said user.

38. A controller unit according to any of the claims 33 to 37, comprising additionally an interface unit.

39. A controller unit according to claim 38, wherein said interface unit is connected to an authorized device or an authorized instant.

40. A controller unit according to claim 38 or 39, wherein said interface unit is connected via a transmission network.

41. A controller unit according to claim 40, wherein said transmission network is a wide area transmission network.

42. A controller unit according to claim 40, wherein said transmission network is a local area transmission network.

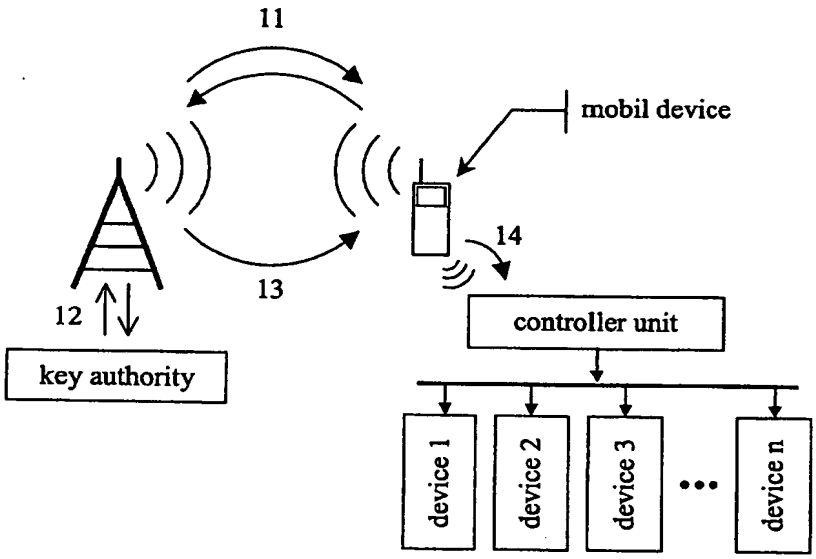

Fig. 1

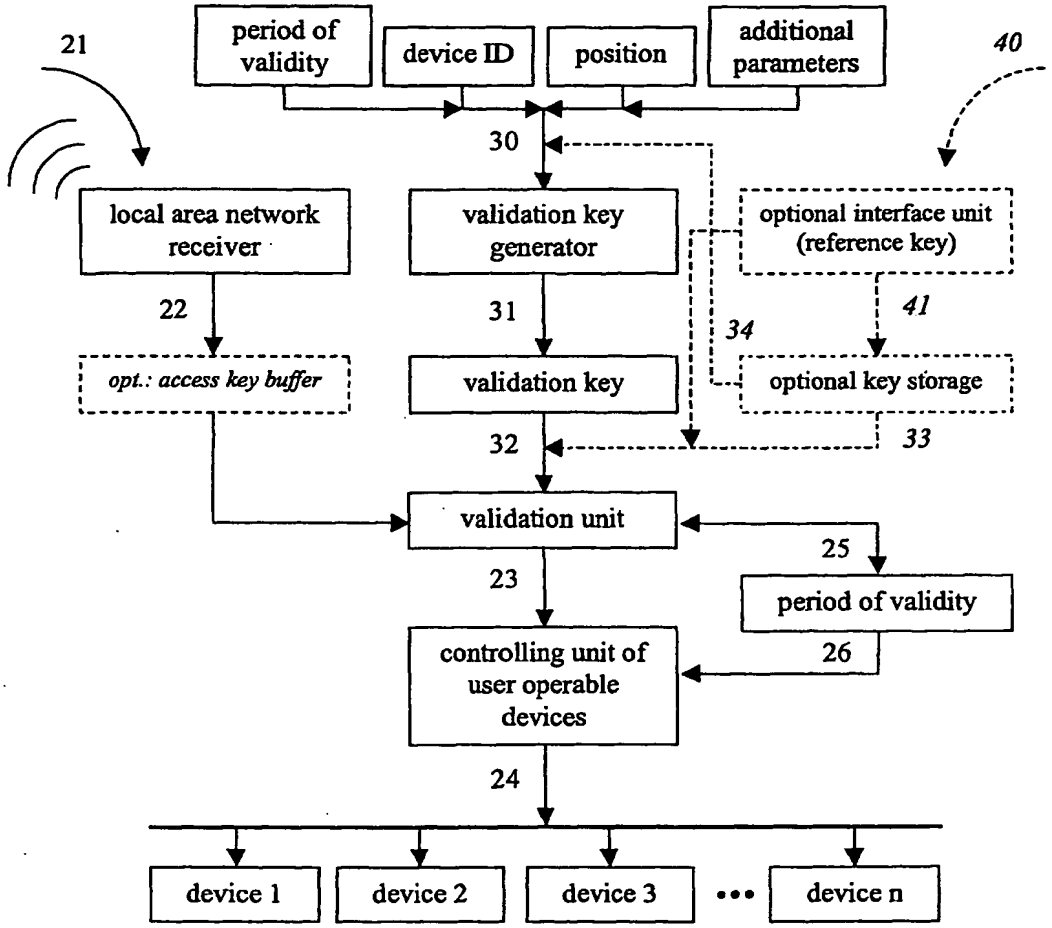
period of validity
device ID
position
additional parameters
21
40
30
local area network receiver
validation key generator
optional interface unit (reference key)
22
31
41
34
opt.: access key buffer
validation key
optional key storage
32
33
validation unit
25
23
period of validity
26
controlling unit of user operable devices
24
device 1
device 2
device 3
device n

Fig. 2

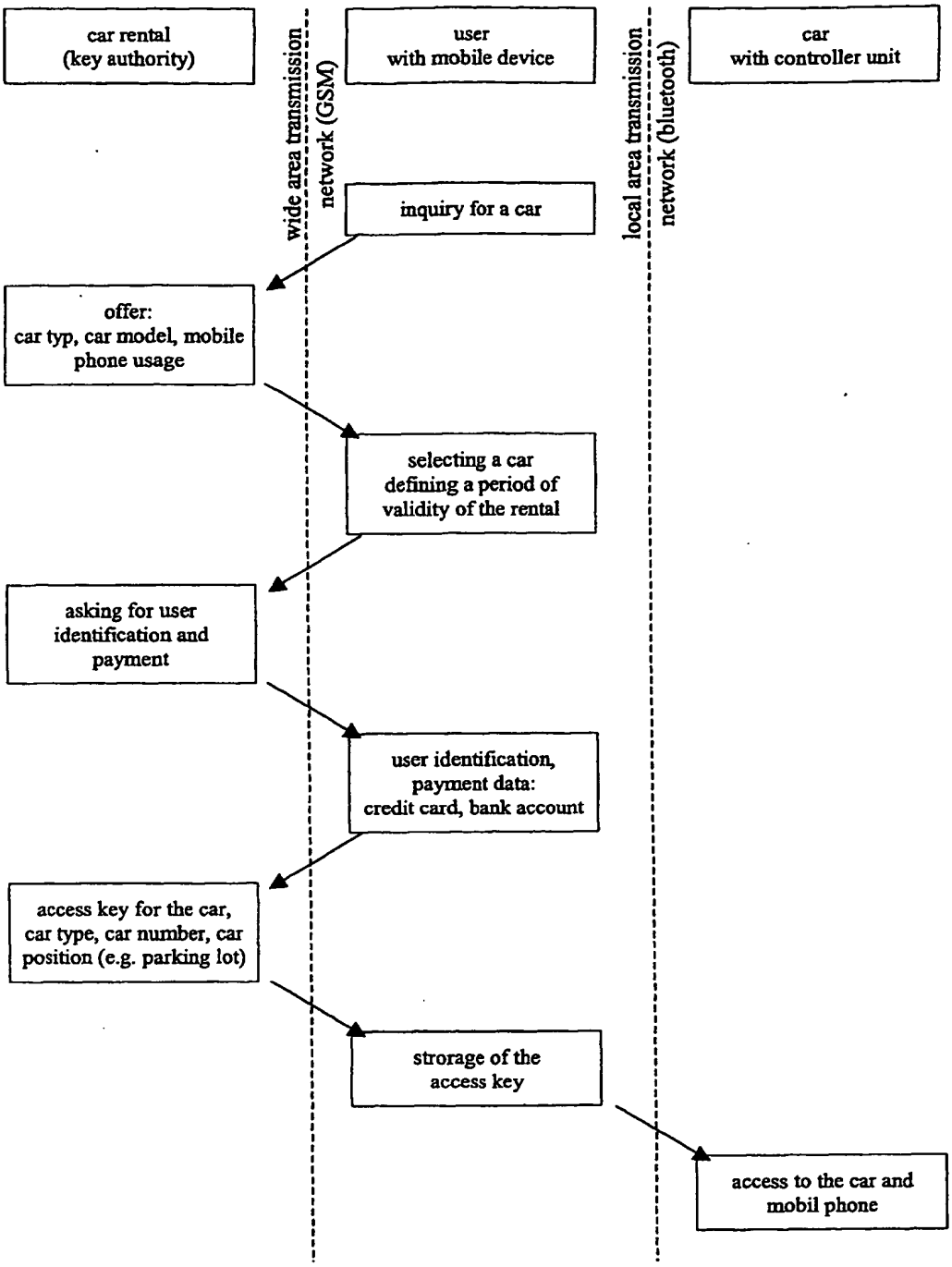

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 11 5474

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 01 40605 A (NIELSEN ERNST LYKKE ;BORDING DATA AS (DK)) 7 June 2001 (2001-06-07) * abstract * * page 22, line 21 - page 23, line 5 * * page 25, line 1 - page 26, line 28 * * page 29, line 10 - line 30 * * page 32, line 11 - page 36, line 2 * * figures 2,6,7 * ---	1-6,10, 11, 13-25, 27-30, 32-42	G07C9/00 G07B15/00
X	US 6 175 922 B1 (WANG YNJIUN P) 16 January 2001 (2001-01-16) * column 17, line 50 - column 20, line 34 * * figures * ---	1-4, 6-13, 20-22, 24, 26-29, 31-33, 35,38-42	
E	WO 01 63425 A (ERICSSON TELEFON AB L M) 30 August 2001 (2001-08-30) * page 6, line 1 - page 12, line 9 * * figures * ---	1,4-13, 20-27, 31-35, 38-42	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07C G07B E05B
A	US 5 705 991 A (WELLS III RALPH H ET AL) 6 January 1998 (1998-01-06) * column 7, line 22 - column 8, line 7 * * figure 3 * ---	1,27,33	
A	EP 0 410 024 A (SIEMENS AG) 30 January 1991 (1991-01-30) * abstract; claims; figures * --- -/--	1,27,33, 37	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	27 November 2001	Miltgen, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 11 5474

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	WO 98 25000 A (BROOKS CO E J) 11 June 1998 (1998-06-11)		

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	27 November 2001	Miltgen, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 11 5474

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-11-2001

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0140605	A	07-06-2001	AU	1513201 A	12-06-2001
			AU	1513301 A	12-06-2001
			WO	0140605 A1	07-06-2001
			WO	0141075 A1	07-06-2001
US 6175922	B1	16-01-2001	US	6282656 B1	28-08-2001
			US	5917913 A	29-06-1999
			WO	0169388 A1	20-09-2001
			AU	5383198 A	29-06-1998
			WO	9825371 A1	11-06-1998
WO 0163425	A	30-08-2001	NO	20000941 A	27-08-2001
			WO	0163425 A1	30-08-2001
US 5705991	A	06-01-1998	US	6072402 A	06-06-2000
			AT	155912 T	15-08-1997
			AU	691137 B2	07-05-1998
			AU	1229497 A	13-03-1997
			AU	2589492 A	03-08-1993
			BR	9207033 A	05-12-1995
			DE	69221165 D1	28-08-1997
			DE	69221165 T2	27-11-1997
			EP	0639287 A1	22-02-1995
			ES	2106883 T3	16-11-1997
			HK	1001598 A1	26-06-1998
			JP	2894515 B2	24-05-1999
			JP	7502871 T	23-03-1995
			WO	9314571 A1	22-07-1993
			US	5475375 A	12-12-1995
			US	5815557 A	29-09-1998
			US	5654696 A	05-08-1997
EP 0410024	A	30-01-1991	EP	0410024 A1	30-01-1991
			DE	58908418 D1	27-10-1994
WO 9825000	A	11-06-1998	AU	5687798 A	29-06-1998
			EP	0958444 A1	24-11-1999
			WO	9825000 A1	11-06-1998
			US	6317025 B1	13-11-2001
			US	6097306 A	01-08-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82